CLAIMS

What is claimed is:

1. A method for evaluating the security of a cryptographic device to recover useful information about a key, said device containing at least said key and a circuit configured to perform cryptographic operations using said key, said method comprising:

(a) connecting said device to an analog-to-digital converter configured to measure an attribute related to operation of said device;

(b) sending a plurality of command sequences to said device, where each said command sequence causes said device to perform a cryptographic operation to process data using said key;

(c) during processing of each said cryptographic operation, recording a plurality of measurements of said attribute by using said analog-to-digital converter; and

(d) determining whether information about said key is leaking from said device by statistically combining said recorded measurements.

2. A method for evaluating the security of a cryptographic device to recover useful information about a key, said device containing at least said key and a circuit configured to perform cryptographic operations using said key, said method comprising:

(a) connecting said device to an analog-to-digital converter configured to measure electromagnetic radiation during operation of said device;

(b) sending a plurality of command sequences to said device, where each said command sequence causes said device to perform a cryptographic operation to process data using said key;

(c) during processing of each said cryptographic operation, recording a plurality of measurements of said radiation by using said analog-to-digital converter; and

(d) determining whether information about said key is leaking from said device by statistically combining said recorded measurements.

3. A method for evaluating the security of a cryptographic device to recover useful information about a key, said device containing at least said key and a circuit configured to perform cryptographic operations using said key, said method comprising:

(a) connecting said device to an analog-to-digital converter configured to measure an amount of power consumed on an external power input to said device;

(b) sending a plurality of command sequences to said device, where each said command sequence causes said device to perform a cryptographic operation to process data using said key;

(c) during processing of each said cryptographic operation, recording a plurality of measurements of said power by using said analog-to-digital converter; and

(d) determining whether information about said key is leaking from said device by statistically combining said recorded measurements.

4. The method of claim 3 where said cryptographic operation includes transforming with a block cipher.

5. The method of claim 4 where said block cipher includes DES.

6. The method of claim 5 where said data includes an input to said DES block cipher operation.

7. The method of claim 5 where said data includes an output from said DES block cipher operation.

8. The method of claim 2 where said step (d) further includes determining information about said key.

9. The method of claim 8 where said information about said key is usable to reduce an amount of effort required for a brute force attack against said key.

10. The method of claim 9 where said information about said key includes values of a plurality of key bits.

11. The method of claim 1 further comprising temporally aligning data points corresponding to a point of interest within said plurality of measurements.

12. A system for evaluating the security of a cryptographic hardware, comprising:

(a) a device containing at least a key and a circuit configured to perform cryptographic operations using said key;

(b) an analog-to-digital converter connected to said device and configured to measure an attribute related to operation of said device;

(c) data storage system configured to record a plurality of measurements of said attribute, where said measurements are taken by said analog-to-digital converter during processing of each said cryptographic operation; and

(d) statistical processing system for combining said measurements to determine whether information about said key is leaking from said device.

13. The system of claim 12 where said attribute includes electromagnetic radiation from said device.

14. The system of claim 12 where said attribute includes variations in an amount of power consumed on an external power input to said device.

15. The system of claim 14 where said cryptographic operation includes transforming using a block cipher.

16. The system of claim 13 where said element (d) is configured to determine information about said key.

17. The system of claim 12 further comprising a data filtering system configured to temporally align data points corresponding to a point of interest within said plurality of measurements.

18. A method for analyzing externally measurable characteristics of a cryptographic device, said device containing a secret key and configured to perform cryptographic operations with said key, to recover information about said key, said method comprising:

(a) connecting said device to an analog-to-digital converter configured to measure said characteristic during operation of said device;

(b) during a said cryptographic operation, using said analog-to-digital converter to measure a plurality of measurements of said attribute;

(c) storing said set of measurements in a memory;

(d) repeating said (b) and (c) a plurality of times to produce a plurality of sets;

(e) computing the alignment of said measurements in said plurality of sets such that measurements corresponding to a single point of interest can be compared;

(f) generating a guess of a value of a portion of said key;

(g) using said guess, computing an average of a subset of said aligned measurements; and

(h) verifying correctness of said guess by detecting existence of a bias in said average.

19. The method of claim 18 where said characteristic is an amount of power consumed on an external power input to said device.